IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

UNITED STATES OF AMERICA,	§	
	§	
Plaintiff,	§	5:17-CR-00626 (1)-OLG
	§	
vs.	§	
	§	
JEFFREY CRAIG MORROW,	§	
	§	
Defendant,	§	

REPORT AND RECOMMENDATION
OF UNITED STATES MAGISTRATE JUDGE

To the Honorable Chief United States District Judge Orlando Garcia:

This Report and Recommendation concerns the Motion to Suppress Evidence and Request for a *Franks v. Delaware* Hearing, filed by Defendant Jeffrey Craig Morrow. *See* Dkt. Nos. 23 & 28 (supporting affidavit). The district court referred the motion to suppress to the undersigned for a Report and Recommendation pursuant to 28 U.S.C. § 636(b)(1)(B) and Western District of Texas Local Rules CR-58 and 1(d) to Appendix C. As discussed below, the undersigned recommends that the motion be denied. Morrow's alternative request for a hearing and relief pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), should likewise be denied because it is moot and, alternatively, fails on the merits.

I. Background

In July of 2015, federal investigators at Homeland Security Investigations identified a specific internet protocol (IP) address that was providing access via the internet, through peer-to-peer software, to files depicting child pornography. Over the course of the next several months—including on August 10, 2015, November 23, 2015, and February 8, 2016—investigators

downloaded *directly* via that same IP address numerous image and video files depicting child pornography.

During the following month, in August of 2015, investigators sought and obtained information about the internet services associated with the specific IP address from the internet-service provider, AT&T. These efforts linked the internet services associated with the target IP address to a physical location in San Antonio, Texas. They also identified the internet-services subscriber as Stephanie Carrier and revealed Defendant Jeffrey Morrow as another individual associated with the internet-services account. Authorities then confirmed the validity of this subscriber and physical-location information for the August 10, 2015, November 23, 2015, and February 8, 2016 dates on which investigators had directly downloaded files depicting child pornography via the target IP address.

By July of 2016, investigators were able to match digital signatures for known child-pornography files held in a law enforcement repository with file signatures associated with the target IP address. In short, federal investigators determined that a device or devices using the target IP address to access the internet during July of 2016 contained these known child-pornography files. The following month, a special agent assigned to the case since early in 2016, Special Agent Juarez, again confirmed that the internet-services-subscription and physical-location information for the internet-services account associated with the target IP address remained unchanged.

Investigators also confirmed the additional information obtained so far. To that end, Special Agent Juarez obtained driver's license photographs for two individuals—Jeffrey Morrow and Stephanie Carrier Morrow—who listed the San Antonio address associated with the target IP address as their residence. Special Agent Juarez then cross-referenced this information with

credit-history information, property records, and public-utility information. And on four separate dates in June and July of 2016, investigators conducted surveillance at the residence now associated with the target IP address. Through these efforts they confirmed that the target IP address was still active at the residence and that Morrow and Carrier still lived there. Special Agent Juarez then, on August 22, 2016, sought a search warrant for the residence.

Agents executed the warrant two days later, on August 24, 2016. Morrow was present when agents executed the warrant, and he made a number of incriminating statements to them in the course of their activities at his residence. He confirmed that AT&T was his internet provider and admitted to using eMule, a peer-to-peer file-sharing program, to download child pornography. As a result of their search, agents seized, among other things, Morrow's desktop computer and three external hard drives. Preliminary forensic examination of the desktop's hard drive and the three external hard drives revealed that they contained files depicting child pornography.

A grand jury indicted Morrow on August 2, 2017, on charges that he received, possessed, and distributed child pornography. On November 3, 2017, Morrow filed his motion to suppress, seeking to suppress all evidence found as a result of the search conducted pursuant to the warrant. *See* Dkt. No. 23. Morrow argues in his motion that the warrant lacks any indicia of probable cause to justify a search of his residence. Specifically, he argues that probable cause is lacking due to the alleged staleness of the information provided therein. *Id.* He further argues that Special Agent Juarez either intentionally or recklessly omitted or misstated allegedly crucial information regarding the precise nature of the undercover investigation and IP addresses in general, as well as the inherent mobility and fungibility of computers and other similar devices.

Id. On December 8, 2017, the undersigned held a hearing on Morrow's motion at which Special Agent Juarez testified.

II. Analysis

Through a number of related and somewhat overlapping arguments, Morrow invokes several alleged omissions and errors in Special Agent Juarez's probable-cause affidavit, which Morrow contends render the warrant invalid and incapable of providing probable cause for the search.

The Fourth Amendment requires that a search warrant be supported by probable cause. It provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and *no Warrants shall issue, but upon probable cause*, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV (emphasis added). Accordingly, under the exclusionary rule, courts "suppress evidence seized on the basis of a warrant that is unsupported by probable cause." *United States v. Pope*, 467 F.3d 912, 916 (5th Cir. 2006) (citing *Mapp v. Ohio*, 367 U.S. 643 (1961)). The exclusionary rule demands suppression of "not only the illegally obtained evidence itself, but also other incriminating evidence derived from that primary evidence." *United States v. Runyan*, 275 F.3d 449, 466 (5th Cir. 2001) (citing *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920)). Thus, "the exclusionary rule encompass[es] evidence that is the indirect product or 'fruit' of the unlawful police conduct." *Id.* (citing *Wong Sun v. United States*, 371 U.S. 471 (1963)).

"The exclusionary rule is not without limits, however." *Id.* One limit, the good-faith exception, is implicated here. *See United States v. Leon*, 468 U.S. 897 (1984).

A. The Good-Faith Exception to the Exclusionary Rule Applies.

Requests to invoke the exclusionary rule and suppress evidence obtained pursuant to a search warrant, like Morrow's, are typically governed by a two-stage test. *See United States v. Mays*, 466 F.3d 335, 342-43 (5th Cir. 2006). At the first stage, a court investigates whether the good-faith exception applies. This involves determining whether "the executing officers' reliance on the warrant was objectively reasonable and in good faith." *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003); *Leon*, 468 U.S. at 921-25. If officers executing the warrant relied on it in good faith, evidence obtained pursuant to the warrant will not be suppressed, even if the warrant is later found invalid. *Payne*, 341 F.3d at 399; *Leon*, 468 U.S. at 921-25. This good-faith inquiry is "'confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.'" *Payne*, 341 F.3d at 399 (quoting *Leon*, 468 U.S. at 922 n. 23). It does not involve an "expedition into the minds of police officers' to determine their subjective belief regarding the validity of the warrant." *Id*. Whether the exception applies "will ordinarily depend on an examination of the affidavit by the reviewing court," *United States v. Gant*, 759 F.2d 484, 487-88 (5th Cir.1985), but "all of the circumstances [surrounding the warrant's issuance] may be considered." *Leon*, 468 U.S. at 922 n. 23.

At stage two, courts determine whether the warrant is supported by probable cause. But if there is a finding of good faith at stage one, "the stage two question of probable cause for the warrant" need not be addressed at all, "unless it presents a 'novel question of law,' resolution of which is 'necessary to guide future action by law enforcement officers and magistrates.'" *Payne*, 341 F.3d at 399 (quoting *Leon*, 468 U.S. at 925). Here, the officers' reliance on the warrant was

objectively reasonable and in good faith, and, in the view of the undersigned, the inquiry properly ends at stage one with that conclusion.

A reasonably well-trained officer executing the warrant in this case would not have had any reason to question the legality of the search. The warrant and accompanying affidavit detail the direct download of child-pornography files by federal agents via the specific IP address associated with the residence properly identified for search in the warrant. Indeed, the warrant's affidavit details that:

- Law-enforcement officers were conducting undercover investigations using peer-to-peer software to find individuals trafficking in child pornography.
- Investigators identified the specific target IP address at issue in this case as one providing access to child pornography for download via peer-to-peer software.
- From August 2015 through at least February 2016, investigators *directly downloaded* numerous child-pornography files from a device connected to the internet via the target IP address.
- In July 2016, the digital signatures of files downloaded via the target IP address were matched with digital signatures of files maintained in a law-enforcement repository and previously identified as child pornography.
- The target IP address was assigned to a specific residential address, which the warrant targeted for search, both at the time investigators downloaded child pornography via the IP address and up to and including the date of the warrant's execution.
- Internet-service-provider-account information directly connected Defendant Morrow with the IP address by specifically listing him as a person associated with the account.
- Morrow was associated with the physical address for the IP address in driver's license information as well as credit-history information and property records.
- Investigators personally witnessed Morrow at the physical address.

Accordingly, a "'reasonably well trained officer would [not] have known that the search was [somehow] illegal despite the magistrate's authorization.'" *Payne*, 341 F.3d at 399. The above-

listed items detailed in the affidavit, and not meaningfully challenged by Morrow, establish that official reliance on the affidavit and warrant was entirely reasonable and in good faith.

B. The Circumstances Presented Are Not Such That the Good-Faith Exception Cannot Apply.

Urging suppression of all evidence seized pursuant to the search warrant, Morrow argues that four errors or omissions in the affidavit supporting the warrant render the warrant invalid. Specifically, he argues the affidavit:

(1) misled the issuing magistrate judge about the staleness of investigative information, Mot. at 3, 11-18, 25-26;

(2) failed to acknowledge the "inherent mobility, fungibility, or ease of transport of computers, laptops, tablets and cell phones," *id.* at 3, 9, 24, 25-26;

(3) erroneously and misleadingly linked the target IP address to a specific computer, *id.* at 3, 22-26; and

(4) did not disclose precisely how authorities identified the target IP address as one connected with child-pornography activity, *id.* at 3, 19-22, 25-26.

These alleged errors or omissions in the affidavit, Morrow contends, misled the magistrate judge who issued the warrant, ultimately yielding a warrant that "no reasonable law enforcement professional could claim to have relied on [ ] in good faith." *Id.* at 24.

Morrow's arguments implicate two sets of circumstances in which the "good faith exception cannot apply." *Leon*, 468 U.S. at 923 (listing four types of circumstances in total, including the two at issue here); *Payne*, 341 F.3d at 399-400. The first set of circumstances addresses situations in which "the issuing magistrate/judge was misled by information in an affidavit that the affiant knew was false or would have known except for reckless disregard of the truth." *Payne*, 341 F.3d at 399-400 (internal quotation marks omitted). This "exception" to the good-faith exception, therefore, touches on the affiant's subjective good faith. The second set of circumstances potentially at issue here describes the extreme situation "where the warrant is

based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id*. (internal quotation marks omitted). As demonstrated by the discussion above detailing unchallenged matters in the affidavit, Morrow cannot advance a winning argument that the affidavit here so lacks the indicia of probable cause that official belief in it would be entirely unreasonable. *See* Section D *infra* (discussing the probable cause standard and its application here).

Moreover, in either of these two sets of circumstances suppression is not warranted unless the information implicated by the affidavit's alleged deficiency is itself necessary to the probable-cause determination. *See Franks*, 438 U.S. at 171; *United States v. Dickey*, 102 F.3d 157, 161-62 (5th Cir. 1996); *United States v. Davis*, 226 F.3d 346, 351 (5th Cir. 2000). In other words, even where a defendant makes a "'showing of deliberate falsity or reckless disregard for the truth by law enforcement officers, he is not entitled to a [*Franks*] hearing'" (which delves into the affiant's actions), let alone to ultimately suppress evidence obtained pursuant to the warrant, if the "'subject of the alleged falsity or reckless disregard is set to one side[] [and] there remains sufficient content in the warrant affidavit to support a finding of probable cause.'" *Dickey*, 102 F.3d at 161 (quoting *United States v. Privette*, 947 F.2d 1259, 1261 (5th Cir.1991)). Thus, although the "falsehood can be perpetrated by omission as well as commission," if the defendant invokes an omission in the affidavit, then that "omission must be of information that is not only relevant, but dispositive, so that if the omitted fact were included, there would not be probable cause." *Davis*, 226 F.3d at 351-52.

The errors or omissions Morrow invokes, even if proven, could not require the suppression of evidence because, as discussed below, those alleged deficiencies do not involve matters necessary or dispositive to a probable-cause finding in this case.

1. The supposed staleness of investigative information does not render the good-faith exception inapplicable.

Morrow contends Special Agent Juarez intentionally or recklessly misled the magistrate judge by failing to fully disclose a 6-month gap between the final time in February of 2016 that investigators downloaded child pornography and the date they sought the search warrant. Mot. at 23-25. This gap, according to Morrow, rendered the investigative information stale, a fact Morrow contends Special Agent Juarez should have disclosed to the magistrate judge. This argument fails because the 6-month gap did not render the investigative information stale. It also fails because the supposed staleness of information was not necessary or dispositive to a probable-cause determination, and, finally, it additionally fails because Special Agent Juarez did not intentionally or recklessly mislead the magistrate judge.

"The amount of delay which will make information stale depends upon the particular facts of the case, including the nature of the criminal activity and the type of evidence sought." *United States v. Allen*, 625 F.3d 830, 842 (5th Cir. 2010). Although Morrow contends he is raising a novel issue of law, the case law addressing staleness in child-pornography investigations belies his contention. Indeed, "[a] number of courts have considered the issue of whether information in a child pornography case is stale for the purposes of determining whether there was probable cause for the issuance of a warrant." *Id.* at 842-43 (discussing a number of staleness cases in the child-pornography context); *United States v. Silva*, No. SA–09–CR–203–XR, 2009 WL 1606453 at *6 (W.D. Tex. Jun. 8, 2009) ("Information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned."). These cases and the principles discussed in them reflect that Morrow's 6-month period is insufficient to show staleness under the facts presented here.

The nature of the criminal activity and type of evidence sought are sufficiently similar here to that in *Allen* and the decisions cited and discussed in it to guide the analysis here. As noted in *Allen*, crimes involving child pornography are "generally carried out in the secrecy of the home and over a long period; therefore the same time limitations that apply to more fleeting crimes do not apply to child pornography cases." *Allen*, 625 F.3d at 843 (citing *United States v. Frechette*, 583 F.3d 374, 378-79 (6th Cir. 2009)). As courts have previously noted, "[g]iven the complex nature of child pornography investigations, the evidence may take several months or years to accrue, and that evidence may consist of bits and pieces from camouflaged sources." *Silva*, 2009 WL 1606453, at *6. *Allen* discusses various child-pornography cases involving digital files and other media, and it addresses periods including 5 years, 3 years, 16 months, 10 months, and 13 months as all being insufficient to render investigative information stale in this context. *Allen*, 625 F.3d at 843. *Allen* itself involved a period of 18 months, which the Fifth Circuit affirmed was insufficient to render the investigative information stale. *See also United States v. Winkler*, No. SA-07-CR-253-XR, 2008 WL 859197, at *5-7 (W.D. Tex. Mar. 28, 2008) (13-month period did not result in staleness in child-pornography case).

The nature of the digitally stored evidence sought here is akin to that at issue in *Allen*, as is the nature of the alleged criminal activity. The 6-month period here is a third of the gap found insufficient to show staleness in *Allen*. The investigative information here, in short, was not stale.

Further, as in *Allen*, it was reasonable for the magistrate judge here to conclude under the totality of circumstances presented that pornographic images could be found on one or more electronic devices at the target physical address and to conclude, more generally, that "there [wa]s probable cause to believe that the fruits, instrumentalities or evidence of criminal acts exist[ed] at the place for which the warrant [wa]s requested." *Allen*, 625 F.3d at 842. Indeed, a

magistrate judge need only have a substantial basis to conclude that a search would uncover evidence of a crime, which is a standard more than satisfied here. *See United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (citing *United States v. Brown*, 941 F.2d 1300, 1302 (5th Cir. 1991)). The alleged staleness of information, in other words, was not material to the probable-cause determination, let alone dispositive of it.

Moreover, the undersigned finds that Special Agent Juarez did not mislead the magistrate, or submit a false statement in her affidavit knowingly and intentionally, or with reckless disregard for the truth, including by way of omission. Special Agent Juarez testified at the hearing on the motion to suppress, and in so doing credibly refuted any suggestion that she knowingly and intentionally, or recklessly misled the magistrate judge about any matters addressed in her affidavit. Further, her affidavit includes a timeline of the investigation, and it relates the February 2016 date of the last direct download via the target IP address. To the extent the timeline may or may not be entirely clear about whether and to what extent other files were downloaded or accessed after that date and before issuance of the warrant, that alleged lack of clarity falls far short of reflecting a reckless disregard for the truth. Given that the 6-month period at issue is not necessary to a probable-cause determination here, any possible minor error or oversight in the affidavit's description of the investigation's timeline cannot have been made with reckless disregard for the truth and, ultimately, could not be said to have misled anyone.

In sum, the investigative information at issue here was not stale, and any alleged failure by the affiant to disclose the 6-month gap was not necessary or dispositive to a probable-cause determination. The special agent did not mislead the magistrate judge, either intentionally or with reckless disregard for the truth. Finally, any alleged staleness could not have rendered the

affidavit and warrant so lacking in any indicia of probable cause as to render official belief in it unreasonable.

2. Alleged erroneous references to "a computer" in the affidavit and omissions concerning the fungibility, mobility, and interchangeability of devices do not render the good-faith exception inapplicable.

Morrow's next two arguments make the most sense when taken together, and so they will be discussed together here. He argues that the affidavit omitted a necessary explanation of the inherent mobility, fungibility, and ease of transport of computers and other electronic devices and, relatedly, that the affidavit also mistakenly and misleadingly linked the target IP address to a specific computer, as opposed to a network, associated with Morrow's residence. The upshot, according to Morrow, is that without sufficient discussion of these matters, a magistrate judge could not accurately make the necessary connection between the investigative evidence showing downloads of pornographic materials via the target IP address and any devices likely to be found at the residence targeted for search.

As noted above, crimes involving child pornography are "generally carried out in the secrecy of the home and over a long period." *Allen*, 625 F.3d at 843. Moreover, as Special Agent Juarez's affidavit details, many individuals who use child pornography also collect and store it on a variety of media that they keep readily at hand, usually in their residence.[1] This feature is

[1] Attachment C to Ex. 1 of Mot. ¶ 24.1 ("Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media."); *id*. ¶ 24.3 ("[I]ndividuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence . . .").

recognized in decisions addressing requests to suppress evidence in child-pornography cases.[2] As for the term "computer," it is specifically defined in the affidavit. That term, as used in the affidavit, "includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware." Attachment B to Ex. 1 of Mot., at 4. These considerations reflect that the probable-cause determination did not materially involve whether a specific computer had been identified as containing suspect files, or whether multiple devices could or could not access the IP address and be moved or interchanged. Instead, the totality of circumstances reflects that the "magistrate had a substantial basis for concluding 'that a search would uncover evidence of wrongdoing'" because the IP address used for unlawful activity was associated with a physical address where evidence and instrumentalities of that criminal activity could reasonably be expected to be found. *Diaz*, 529 F. Supp. at 794 (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)).

Moreover, there are ample grounds to find probable cause for a search of the residence even if all references to "the computer" were removed from or were perfectly clarified in the affidavit. The same is true regarding alleged omissions about the mobility and fungibility of electronic devices and similar matters. There was ample *additional, independent* investigative

[2] *See, e.g.*, *Allen*, 625 F.3d at 843; *United States v. Whisman*, No. 416CR00173MACCAN, 2018 WL 459342, at *9 (E.D. Tex. Jan. 5, 2018), report and recommendation adopted sub nom., 2018 WL 454248 (E.D. Tex. Jan. 17, 2018) (recognizing that a defendant can save and store child pornography on any form of digital media—CDs, DVDs, flash drives, disconnected hard drives, etc.) (citing *United States v. Farlow*, 681 F.3d 15, 18-19 (1st Cir. 2012)); *United States v. Brunson*, MO-09-CR-238, 2010 WL 11545746, at *5 (W.D. Tex. Jan. 28, 2010) (explaining that "[e]stablishing particularity under a child pornography warrant presents a unique challenge for law enforcement because child pornography can be stored electronically in a variety of storage devices"); *United States v. Diaz*, 529 F. Supp. 2d 792, 797 (S.D. Tex. 2007) ("Collectors of child pornography typically maintain and possess child pornography in secure locations, 'most often at a residence or other secure location.'") (quoting affidavit).

evidence to support probable cause for a search. For example, the router, modem, and other network equipment at the home were the instrumentalities of a crime, which could be targeted for seizure based on a probable-cause determination that they were used to download and share child-pornography files. *See, e.g.*, *Wallace v. Wellborn*, 204 F.3d 165, 167 (5th Cir. 2000) ("The general rule under the Fourth Amendment is that any and all contraband, instrumentalities, and evidence of crimes may be seized based on probable cause.") (citing *Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 62-63 (1989)). In the end, vastly more than a fair probability that evidence, instruments, or contraband from the commission of a crime could be found at the residence is shown here, even if Morrow's alleged errors or omissions are taken completely out of the probable-cause picture.

Finally, as already noted, Special Agent Juarez did not mislead the magistrate, or submit a false statement in her affidavit knowingly and intentionally, or with reckless disregard for the truth, including by way of omission.

In sum, no set of circumstances in which the good-faith exception could not apply is satisfied by Morrow's arguments about the mobility or fungibility of electronic devices or the affidavit's references to "the computer."

3. The affidavit's omission of investigative details does not render the good-faith exception inapplicable.

A similar analysis applies to Morrow's final attempt to sidestep the good-faith exception, in which he invokes the affidavit's alleged failure to discuss fully all details of the investigation that led to the target IP address. Morrow specifically takes issue with the affidavit's failure to divulge the nature of the computer software used to identify the target IP address. He contends that without disclosing this information to the magistrate judge, there was no way for the probable-cause determination to take into account the reliability or other features of that

software.[3] Again, because this omitted investigative detail is not even close to being material or dispositive on the probable-cause determination here, it cannot justify the suppression of evidence. *See Davis*, 226 F.3d at 351-52 (to support the suppression of evidence even an intentional falsehood "perpetrated by omission" "must be of information that is not only relevant, but dispositive, so that if the omitted fact were included, there would not be probable cause").

Given the totality of circumstances, including all the investigative evidence connecting the target IP address with child pornography and Morrow, there was more than a sufficient basis to find probable cause for the search, notwithstanding any error or omission in the affidavit involving how investigators came upon Morrow's IP address. Probable cause involves a flexible, common-sense standard that ultimately is concerned with determining under the totality of circumstances whether a person of reasonable prudence would believe evidence, contraband, or the instruments of a crime will be found. *Ornelas v. United States*, 517 U.S. 690, 696 (1996); *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006) ("Probable cause exists when there are reasonably trustworthy facts which, given the totality of the circumstances, are sufficient to lead a prudent person to believe that the items sought constitute fruits, instrumentalities, or evidence of a crime."). It simply stretches too far to say, as Morrow does, that the magistrate judge's probable-cause determination here turned on the undisclosed details of the software authorities used to identify his IP address as one engaging in illegal activity. This is not a case where

[3] Notably, Morrow does not argue that the process by which agents used to identify the target IP address was itself an unlawful search or seizure. *See* Mot. at 4 ("The Defendant does not assert at this time that the utilization of CPS violates the Fourth Amendment nor that individuals have an expectation of privacy on [peer-to-peer] Networks."). Nor would such an argument have merit. *See United States v. Weast*, 811 F.3d 743, 748 (5th Cir. 2016) (holding that there is no reasonable expectation of privacy in an IP address or files shared through peer-to-peer software).

authorities used an unexplained "tip" from certain software as the *only basis* to justify a search.[4] Rather, here there was ample *other independent* investigative information that supports a probable-cause determination, including (but not limited to) the direct receipt of child-pornography via the target IP address associated with the physical address and the matching of files known to contain child pornography with files on a device using the target IP address.[5]

Further, there is simply no evidence that the affiant's failure to mention this investigative detail was a knowing or intentional falsehood, or was made with reckless disregard to the truth. Indeed, given the totality of the circumstances and body investigative evidence gathered and related in the affidavit, the omission of this detail, which is not dispositive of the probable-cause determination, is effectively beside the point. It certainly could not be said to have misled the experienced magistrate judge in this case.

Ultimately, the good-faith exception applies here. The alleged matters in Special Agent Juarez's affidavit about which Morrow complains are not necessary or dispositive to the probable-cause determination, either taken individually or collectively. Morrow fails to show any

---

[4] *Cf. Gates*, 462 U.S. at 267-68 ("[A]n affidavit based on an informer's tip, standing alone, cannot provide probable cause for issuance of a warrant unless the tip includes information that apprises the magistrate of the informant's basis for concluding that the contraband is where he claims it is (the 'basis of knowledge' prong), and the affiant informs the magistrate of his basis for believing that the informant is credible (the 'veracity' prong)") (quotation marks omitted).

[5] *See id.* (noting that even where "an informer's tip, standing alone" is used to support probable cause for a warrant, "probable cause may yet be established by independent police investigatory work that corroborates the tip to such an extent that it supports "both the inference that the informer was generally trustworthy and that he made his charge on the basis of information obtained in a reliable way.") (quotation marks omitted); *see also United States v. Shugart*, 117 F.3d 838, 844 (5th Cir. 1997) (affidavit that related information from confidential informant provided sufficient indicia of probable cause where the government did not exclusively rely on the informant's corroborated allegations but instead conducted an independent investigation to corroborate the information) (citing *J.E.B. v. Alabama ex rel T.B.*, 511 U.S. 127 (1994) (holding that information supplied by a confidential informant, which was corroborated by other evidence, supported a magistrate judge's finding of probable cause, despite a lack of evidence regarding the informant's reliability or veracity)).

circumstances that warrant suppressing evidence on the basis that the good-faith exception could not or should not for some reason apply in this case.

C. Morrow's Request for a *Franks* Hearing Is Moot and, in any Event, Without Merit.

Morrow argues that the same errors and omissions in the supporting affidavit entitle him to an evidentiary hearing under *Franks* and, ultimately, render the affidavit and warrant incapable of supporting a finding of probable cause. Morrow's request for a *Franks* hearing is moot because the undersigned already conducted an evidentiary hearing at which Morrow was permitted to cross-examine Special Agent Juarez on her good-faith in securing a search warrant from a magistrate judge.

Even if the issue of *Franks* hearing were not moot, Morrow would not be entitled to such a hearing because he failed to make the requisite showing. It is only "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, [that] the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks*, 438 U.S. at 156-57. Here, Morrow made no substantial showing that "a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *Id*. And he also made no substantial showing that the "allegedly false statement is necessary to the finding of probable cause." *Id*. As to the first required showing, Special Agent Juarez testified credibly at the hearing, as mentioned previously, and based on her testimony and the other evidence there is no reason on this record to conclude that she either intentionally and knowingly submitted a false statement in her affidavit or omitted from it any necessary or material information. Nor did she do either of those things with a reckless disregard for the truth.

As to the second required showing, for all the reasons discussed above in Section B, Morrow cannot show that any allegedly false statement or omission was necessary to the finding of probable cause.

D. There Is More Than Ample Evidence Here to Support a Finding of Probable Cause.

Finally, although it is not necessary to examine the probable-cause issue here because the good-faith exception applies and Morrow has raised no novel question of law, there nonetheless was probable cause to support the warrant and search here. As mentioned, probable cause "exists when there are reasonably trustworthy facts which, given the totality of the circumstances, are sufficient to lead a prudent person to believe that the items sought constitute fruits, instrumentalities, or evidence of a crime." *Kohler*, 470 F.3d at 1109. As discussed at length above in Sections A and B, there are more than sufficient reasonably trustworthy facts supporting the magistrate's determination of probable cause. This is so even if the alleged errors or omissions in the affidavit are taken completely out of the probable-cause equation. In other words, all the reasons discussed above showing that the alleged errors or omissions invoked by Morrow are not necessary to a probable cause determination also establish that there was probable cause here.

Accordingly, Morrow's argument that the affidavit is facially deficient due to its reliance on allegedly stale investigative information is without merit, for all the reasons discussed in Sections A and B, and in particular Section B.1. The same result pertains with respect to Morrow's argument that there was no probable cause because of the affidavit's alleged erroneous references to "the computer" and failure to discuss the mobility and fungibility of electronic devices. *See* Sections A, B, B.2 *supra*. Finally, the affidavit's alleged omission of investigative details, including the omission of a discussion of the peer-to-peer software used by authorities to

identify the target IP address as one potentially involved in illegal activity, is likewise insufficient to call the magistrate judge's probable-cause determination into question. Indeed, that probable cause determination receives significant deference. *Diaz*, 529 F. Supp. 2d at 794 ("A magistrate judge's determination of probable cause should be 'paid great deference by reviewing courts.'") (quoting *Gates*, 462 U.S. at 236). Given the totality of circumstances and body of investigate evidence presented here, the existence of probable cause and the magistrate judge's determination to that effect are not undermined by Morrow's arguments. *See* Sections A, B, B.3 *supra*.

III. Conclusion

Having considered the Defendant's Motion, Dkt. No. 23, the Government's Response, Dkt. No. 30, and the record in this case, including testimony provided at the December 8, 2017 hearing, the undersigned **RECOMMENDS** that the District Court **DENY** Defendant's Motion to Suppress Evidence and Request for a *Franks v. Delaware Hearing*, Dkt. No. 23.

Instructions for Service and Notice of Right to Object/Appeal

The United States District Clerk shall serve a copy of this report and recommendation on all parties by either (1) electronic transmittal to all parties represented by attorneys registered as a "filing user" with the clerk of court, or (2) by mailing a copy by certified mail, return receipt requested, to those not registered. Written objections to this report and recommendation must be filed **within fourteen (14) days** after being served with a copy of same, unless this time period is modified by the district court. 28 U.S.C. § 636(b)(1). The party shall file the objections with the clerk of the court, and serve the objections on all other parties. A party filing objections must specifically identify those findings, conclusions, or recommendations to which objections are being made and the basis for such objections; the district court need not consider frivolous,

conclusive or general objections. A party's failure to file written objections to the proposed findings, conclusions, and recommendations contained in this report shall bar the party from a *de novo* determination by the district court. *Thomas v. Arn*, 474 U.S. 140, 149-52 (1985); *Acuña v. Brown & Root, Inc.*, 200 F.3d 335, 340 (5th Cir. 2000). Additionally, failure to timely file written objections to the proposed findings, conclusions, and recommendations contained in this report and recommendation shall bar the aggrieved party, except upon grounds of plain error, from attacking on appeal the unobjected-to proposed factual findings and legal conclusions accepted by the district court. *Douglass v. United Servs. Auto. Ass'n*, 79 F.3d 1415, 1428-29 (5th Cir. 1996) (en banc).

IT IS SO ORDERED.

SIGNED this 26th day of January, 2018.

RICHARD B. FARRER
UNITED STATES MAGISTRATE JUDGE